EXHIBIT
U

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

SRI INTERNATIONAL, INC., a California Corporation, Plaintiff, v. INTERNET SECURITY SYSTEMS, INC., a Delaware corporation, INTERNET SECURITY SYSTEMS, INC., a Georgia corporation, and SYMANTEC CORPORATION, a Delaware corporation, Defendants.	Case No. 04-1199-SLR

SUPPLEMENTAL RESPONSES AND OBJECTIONS OF ISS-GA AND ISS-DE TO SRI'S INTERROGATORY NOS. 6 AND 11

Pursuant to Federal Rules of Civil Procedure 26 and 33, Defendants Internet Security Systems, Inc. ("ISS-GA"), a Georgia corporation, and Internet Security Systems, Inc. ("ISS-DE"), a Delaware corporation, (collectively, "ISS") supplement their responses to Plaintiff SRI International, Inc.'s ("SRI's") Interrogatories Nos. 6 and 11.

GENERAL RESPONSES

1. ISS's responses are made to the best of ISS's present knowledge, information and belief. ISS's responses are subject to amendment and supplementation should future investigation indicate that amendment or supplementation is necessary. ISS undertakes no obligation, however, to supplement or amend these responses other than as required by the Federal Rules of Civil Procedure and the Local Rules for the United States District Court for the District of Delaware.

2. ISS's responses are made according to information currently in ISS's possession,

- Tcpdump
- TCP Wrapper
- TIS Firewall Toolkit
- Tivoli Enterprise Manager
- Wisdom & Sense

PRIOR ART REFERENCES THAT INVALIDATE THE CLAIMS-AT-ISSUE

The prior art invalidates the claims at issue under 35 U.S.C. §102 and/or 103, as set forth in detail in the representative charts attached as Exhibits 1-23 to this supplemental response. The cover page of each chart provides citations to referenced prior art, as well as citations to related prior art disclosures. These invalidity charts include:

- Exhibit 1: SRI's Emerald – NISSC (October 9, 1997)
- Exhibit 2: SRI's Emerald – CMAD Workshop, Monterey, 12-14 November 1996.
- Exhibit 3: SRI's Emerald – Conceptual Overview
- Exhibit 4: SRI's Emerald – Conceptual Design and Planning
- Exhibit 5: SRI's Emerald – *Live Traffic Analysis of TCP/IP Gateways*
- Exhibit 6: SRI's Nides/Network Nides
- Exhibit 7: Ji-Nao
- Exhibit 8: NSM
- Exhibit 9: DIDS
- Exhibit 10: ISM
- Exhibit 11: GRIDS
- Exhibit 12: NetRanger
- Exhibit 13: RealSecure

- Exhibit 14: Network Flight Recorder
- Exhibit 15: NetStalker and HP OpenView
- Exhibit 16: HP OpenView and the internet standards
- Exhibit 17: Network Level Intrusion Detection
- Exhibit 18: U.S. Patent No. 5,825,750
- Exhibit 19: Fault Detection in an Ethernet Network via anomaly detectors
- Exhibit 20: Stake Out
- Exhibit 21: Emerald 1997, NSM and NIDES 1994
- Exhibit 22: AIS: Automated Information System
- Exhibit 23: Summary chart of other relevant art

THE CLAIMS-AT-ISSUE ARE INVALID PURSUANT TO 35 U.S.C. § 112

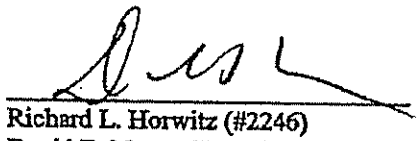
The claims-at-issue are also invalid under 35 U.S.C. § 112 for failure to satisfy the best mode requirement. SRI submitted source code in an Appendix to the patents-in-suit. A preliminary examination of that code indicates that it is not a complete program and could not compile and run. The Appendix appears to lack configuration files that would relate specifically to network traffic data or analysis. The code also does not have code for a resolver. On information and belief, ISS believes discovery will show that SRI had a more complete set of source code by the time it filed U.S. Patent Application No. 09/188,739 and withheld much of that code from the Patent Office. That withheld code reflected the inventor's best mode of practicing the claims at issue.

Similarly, on information and belief, Mr. Porras and Mr. Jou were both present at an Intrusion Detection PI meeting in Savannah, Georgia on February 25-27, 1997. (ISS 27539-27543). On information and belief, Mr. Porras was present at the session where Mr. Jou provided a project update for "Scalable Intrusion Detection for the Emerging Network Infrastructure," again the same title as the invalidating references describing the Ji-Nao system attached as Exhibit 7.

Had the named inventors and/or their agents made accurate representations to the U.S. Patent Office concerning Ji-Nao and disclosures relating to the Ji-Nao project, the patents-in-suit would not have issued. On information and belief, the omissions of the referenced Ji-Nao material were made with an intent to deceive. Thus, those patents are unenforceable due to inequitable conduct.

November 15, 2005

POTTER ANDERSON & CORROON LLP



Richard L. Horwitz (#2246)
David E. Moore (#3983)
Hercules Plaza, 6th Floor
1313 N. Market Street
Wilmington, DE 19899
Tel.: (302) 984-6000
Fax: (302) 658-1192

OF COUNSEL:

Holmes J. Hawkins III
Natasha H. Moffitt
KING & SPALDING LLP
191 Peachtree Street

Atlanta, GA 30303
Tel: (404) 572-4600
Fax: (404) 572-5145

Theresa A. Moehlman
Jeffrey D. Blake
KING & SPALDING LLP
1185 Avenue of the Americas
New York, New York 10036
Tel.: (212) 556-2100
Fax: (212) 556-2222

Attorneys for Defendant
INTERNET SECURITY SYSTEMS, INC.

Live Traffic Analysis invalidates the indicated claims under 35 U.S.C. § 102(b)

All text citations are taken from: P. Porras and A. Valdes, *Live Traffic Analysis of TCP/IP Gateways*, http://www.sdl.sri.com/projects/emerald/live-traffic.html, Internet Society's Networks and Distributed Systems Security Symposium, Nov. 10, 1997 (ISS 28365-28384)

The text included herein are merely representative samples of the disclosure in the asserted reference. ISS reserves the right to supplement these disclosures.

Similar disclosures and additional related information are contained in the following additional references:

- P. Porras and A. Valdes, Live Traffic Analysis of TCP/IP Gateways, Networks and Distributed Systems Security Symposium, March 1998 (IS 359692-359712)
- P. Porras and P. Neumann, *EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances*, 20th NISSC October 9, 1997 (ISS 2892-2904)
- P. Neumann, P. Porras and A. Valdes, *Analysis and Response for Intrusion Detection in Large Networks*, Summary for CMAD Workshop, Monterey, 12-14 November 1996 (ISS 348257-348258)
- *Analysis and Response for Intrusion Detection in Large Networks*, Summary for CMAD Workshop, Monterey, 12-14 November 1996 (SRI 11022-11026)
- *Analysis and Response for Intrusion Detection in Large Networks*, Summary for Intrusion Detection Workshop, Santa Cruz, 26-28 August 1996 (SRI 11045-11048)

- P. Porras and P. Neumann, *EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances Conceptual Overview*, December 18, 1996 (ISS 44439-44441)

- P. Porras and P. Neumann, CONCEPTUAL DESIGN AND PLANNING for EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances, Version 1.2 May 20, 1997, http://www.csl.sri.com/intrusion.html (SRI 12308-12404)

[illegible]	[illegible]	[illegible]
1	A method of network surveillance, comprising:	*"Specifically, we present techniques to analyze TCP/IP packet streams that flow through network gateways for signs of malicious activity, nonmalicious failures, and other exceptional events. The intent is to demonstrate, by example, the utility of introducing gateway surveillance mechanisms to monitor network traffic. We present this discussion of gateway surveillance mechanisms as complementary to the filtering mechanisms of a large enterprise network, and illustrate the usefulness of surveillance in directly enhancing the security and stability of network operations."* (Abstract) "Mechanisms for parsing and filtering hostile external network traffic [2],[4] that could reach internal network services have become widely accepted as prerequisites for limiting the exposure of internal network assets while maintaining interconnectivity with external networks. The encoding of filtering rules for packet- or transport-layer communication should be enforced at entry points between internal networks and external traffic. Developing filtering rules that strike an optimal balance between the restrictiveness necessary to suppress the entry of unwanted traffic, while allowing the necessary flows demanded for user functionality, can be a nontrivial exercise [3]." (p. 2) "Network monitoring, in the context of fault detection and diagnosis for computer network and telecommunication environments, has been studied extensively by the network management and alarm correlation community [8], [11], [15], [16]. The high-volume distributed event correlation technology promoted in some projects provides an excellent foundation for building truly scalable network-aware surveillance technology for misuse. ... Earlier work in the intrusion-detection community attempting to address the issue of network

		surveillance includes the Network Security Monitor (NSM), developed at UC Davis [6], and the Network Anomaly Detection and Intrusion Reporter (NADIR) [7], developed at Los Alamos National Laboratory (LANL). Both performed broadcast LAN packet monitoring to analyze traffic patterns for known hostile or anomalous activity.[i] Further research by UC Davis in the Distributed Intrusion Detection System (DIDS) [23] and later Graph-based Intrusion Detection System (GRIDS) [25] projects has attempted to extend intrusion monitoring capabilities beyond LAN analysis, to provide multi-LAN and very large-scale network coverage." (p. 3)
	receiving network packets handled by a network entity;	*"Specifically, we present techniques to analyze TCP/IP packet streams that flow through network gateways for signs of malicious activity, nonmalicious failures, and other exceptional events."* (Abstract)
	building at least one long-term and at least one short-term statistical profile from at least one measure of the network packets	"4. Traffic Analysis with Statistical Anomaly Detection SRI has been involved in statistical anomaly-detection research for over a decade [1], [5], [10]. Our previous work focused on the profiling of user activity through audit-trail analysis. Within the EMERALD project, we are extending the underlying statistical algorithms to profile various aspects of network traffic in search of response- or alert-worthy anomalies. The statistical subsystem tracks subject activity via one or more variables called *measures*. The statistical algorithms employ four classes of measures: categorical, continuous, intensity, and event distribution. *Categorical* measures are those that assume values from a categorical set, such as originating host identity, destination host, and port number. *Continuous* measures are those for which observed values are numeric or ordinal, such as number of bytes transferred. Derived measures also track the intensity of activity (that is, the rate of events per unit time) and the ''meta-distribution'' of the measures affected by recent events. These derived measure types are referred to as *intensity* and *event distribution*.

		The system we have developed maintains and updates a description of a subject's behavior with respect to these measure types in a compact, efficiently updated *profile*. The profile is subdivided into short- and long-term elements. The short-term profile accumulates values between updates, and exponentially ages values for comparison to the long-term profile. As a consequence of the aging mechanism, the short-term profile characterizes the recent activity of the subject, where ``recent'' is determined by the dynamically configurable aging parameters used. At update time (typically, a time of low system activity), the update function folds the short-term values observed since the last update into the long-term profile, and the short-term profile is cleared. The long-term profile is itself slowly aged to adapt to changes in subject activity. Anomaly scoring compares related attributes in the short-term profile against the long-term profile. As all evaluations are done against empirical distributions, no assumptions of parametric distributions are made, and multi-modal and categorical distributions are accommodated. Furthermore, the algorithms we have developed require no *a priori* knowledge of intrusive or exceptional activity. A more detailed mathematical description of these algorithms is given in [9], [26]." (pp. 5-6) "Statistical anomaly detection via the methods described above enables EMERALD to answer questions such as how the current anonymous FTP session compares to the historical profile of all previous anonymous FTP sessions. Mail exchange could be similarly monitored for atypical exchanges (e.g., excessive mail relays). Continuing with the example of FTP, we assign FTP-related events to a subject (the login user or ``anonymous''). As several sessions may be interleaved, we maintain separate short-term profiles for each, but may score against a common long-term profile (for example, short-term profiles are maintained for each ``anonymous'' FTP session, but each is scored against the historical profile of ``anonymous'' FTP sessions). The aging mechanism in the statistics

Claim Number	Claim Term	Pertinent Text
		module allows it to monitor events either as the events occur or at the end of the session. We have chosen the former approach (analyze events as they happen), as it potentially detects anomalous activity in a session before that session is concluded." (p. 10)
	the at least one measure monitoring data transfers, errors, or network connections;	"IP traffic represents an interesting candidate event stream for analysis. Individually, packets represent parsable activity records, where key data within the header and data segment can be statistically analyzed and/or heuristically parsed for response-worthy activity. However, the sheer volume of potential packets dictates careful assessment of ways to optimally organize packets into streams for efficient parsing. Thorough filtering of events and event fields such that the target activity is concisely isolated, should be applied early in the processing stage to reduce resource utilization. With respect to TCP/IP gateway traffic monitoring, we have investigated a variety of ways to categorize and isolate groups of packets from an arbitrary packet stream. Individual packet streams can be filtered based on different isolation criteria, such as • *Discarded traffic:* packets not allowed through the gateway because they violate filtering rules.[iii] • *Pass-through traffic:* packets allowed into the internal network from external sources. • *Protocol-specific traffic:* packets pertaining to a common protocol as designated in the packet header. One example is the stream of all ICMP packets that reach the gateway. • *Unassigned port traffic:* packets targeting ports to which the administrator has not assigned any network service and that also remain unblocked by the firewall.

Claim Number	Claim Term	
		• *Transport management messages:* packets involving transport-layer connection establishment, control, and termination (e.g., TCP SYN, RESET, ACK, `[window resize]`). • *Source-address monitoring:* packets whose source addresses match well-known external sites (e.g., connections from satellite offices) or have raised suspicion from other monitoring efforts. • *Destination-address monitoring:* all packets whose destination addresses match a given internal host or workstation. • *Application-layer monitoring:* packets targeting a particular network service or application. This stream isolation may translate to parsing packet headers for IP/port matches (assuming an established binding between port and service) and rebuilding datagrams. In the following sections we discuss how such traffic streams can be statistically and heuristically analyzed to provide insight into malicious and erroneous external traffic. Alternative sources of event data are also available from the report logs produced by the various gateways, firewalls, routers, and proxy-servers (e.g., router syslogs can in fact be used to collect packet information from several products)." (pp. 4-5) "Within the EMERALD project, we generalize these concepts so that components and software such as network gateways, proxies, and network services can themselves be made subject classes. The generated event streams are obtained from log files, packet analysis, and--where required--special-purpose instrumentation made for services of interest (e.g., FTP, HTTP, or SMTP). As appropriate, an event stream may be analyzed as a single subject, or as

		multiple subjects, and the same network activity can be analyzed in several ways. For example, an event stream of dropped packets permits analyses that track the reason each packet was rejected. Under such a scenario, the firewall rejecting the packet is the subject, and the measures of interest are the reason the packet was dropped (a categorical measure), and the rate of dropped packets in the recent past (one or more intensity measures tuned to time intervals of seconds to minutes). Alternatively, these dropped packets may be parsed in finer detail, supporting other analyses where the subject is, for example, the identity of the originating host." (p. 5) "Through satellite session profiling, EMERALD can monitor traffic for signs of unusual activity. In the case of the FTP service, for example, each user who gives a login name is a subject, and ''anonymous" is a subject as well. Another example of a subject is the network gateway itself, in which case there is only one subject. All subjects for the same event stream (that is, all subjects within a subject class) have the same measures defined in their profiles, but the internal profile values are different. As we migrate our statistical algorithms that had previously focused on user audit trails with users as subjects, we generalize our ability to build more abstract profiles for varied types of activity captured within our generalized notion of an event stream. In the context of statistically analyzing TCP/IP traffic streams, profiling can be derived from a variety of traffic perspectives, including profiles of • Protocol-specific transactions (e.g., all ICMP exchanges) • Sessions between specific internal hosts and/or specific external sites

[illegible]	[illegible]	[illegible]
		• Application-layer-specific sessions (e.g., anonymous FTP sessions profiled individually and/or collectively) • Discarded traffic, measuring attributes such as volume and disposition of rejections • Connection requests, errors, and unfiltered transmission rates and disposition Event records are generated either as a result of activity or at periodic intervals. In our case, activity records are based on the content of IP packets or transport-layer datagrams. Our event filters also construct interval summary records, which contain accumulated network traffic statistics (at a minimum, number of packets and number of kilobytes transferred). These records are constructed at the end of each interval (e.g., once per N seconds)." (pp. 6-7) See Section 4.1 "Categorical Measures in Network Traffic" (pp. 7-8) See Section 4.2 "Continuous Measures in Network Traffic" (pp. 8-9) See Section 4.3 "Measuring Network Traffic Intensity" (pp. 9-10) See Section 4.4 "Event Distribution Measures" (p. 10) See Section 4.5 "Statistical Session Analysis" (p. 10)
	comparing at least one long-term and at least one short-term statistical profile; and	"EMERALD's statistical algorithm adjusts its short-term profile for the measure values observed on the event record. The distribution of recently observed values is evaluated against the long-term profile, and a distance between the two is obtained. The difference is compared to a historically adaptive, subject-specific deviation. The empirical distribution of this deviation is transformed to obtain a score for the event. Anomalous events are those whose

Claim number	[illegible]	[illegible]
		scores exceed a historically adaptive, subject-specific score threshold based on the empirical score distribution. This nonparametric approach handles all measure types and makes no assumptions on the modality of the distribution for continuous measures." (p. 7)
	determining whether the difference between the short-term statistical profile and the long-term statistical profile indicates suspicious network activity.	"EMERALD's statistical algorithm adjusts its short-term profile for the measure values observed on the event record. The distribution of recently observed values is evaluated against the long-term profile, and a distance between the two is obtained. The difference is compared to a historically adaptive, subject-specific deviation. The empirical distribution of this deviation is transformed to obtain a score for the event. Anomalous events are those whose scores exceed a historically adaptive, subject-specific score threshold based on the empirical score distribution. This nonparametric approach handles all measure types and makes no assumptions on the modality of the distribution for continuous measures." (p. 7)
2	The method of claim 1, wherein the measure monitors data transfers by monitoring network packet data transfer commands.	See '338 claim 1
3	The method of claim 1, wherein the measure monitors data transfers by monitoring network packet data transfer	See '338 claim 1

Claim number	Claim element	Prior art reference
	errors.	
4	The method of claim 1, wherein the measure monitors data transfers by monitoring network packet data transfer volume.	"In the following sections we discuss how such traffic streams can be statistically and heuristically analyzed to provide insight into malicious and erroneous external traffic. Alternative sources of event data are also available from the report logs produced by the various gateways, firewalls, routers, and proxy-servers (e.g., router syslogs can in fact be used to collect packet information from several products)." (p 5) "Within the EMERALD project, we generalize these concepts so that components and software such as network gateways, proxies, and network services can themselves be made subject classes. The generated event streams are obtained from log files, packet analysis, and--where required--special-purpose instrumentation made for services of interest (e.g., FTP, HTTP, or SMTP). As appropriate, an event stream may be analyzed as a single subject, or as multiple subjects, and the same network activity can be analyzed in several ways. For example, an event stream of dropped packets permits analyses that track the reason each packet was rejected. Under such a scenario, the firewall rejecting the packet is the subject, and the measures of interest are the reason the packet was dropped (a categorical measure), and the rate of dropped packets in the recent past (one or more intensity measures tuned to time intervals of seconds to minutes). Alternatively, these dropped packets may be parsed in finer detail, supporting other analyses where the subject is, for example, the identity of the originating host." (p. 5) "Through satellite session profiling, EMERALD can monitor traffic for signs of unusual activity. In the case of the FTP service, for example, each user who gives a login name is a subject, and ``anonymous" is a subject as well. Another example of a subject is the network gateway itself, in which case there is only one subject. All subjects for the same event stream

		(that is, all subjects within a subject class) have the same measures defined in their profiles, but the internal profile values are different. As we migrate our statistical algorithms that had previously focused on user audit trails with users as subjects, we generalize our ability to build more abstract profiles for varied types of activity captured within our generalized notion of an event stream. In the context of statistically analyzing TCP/IP traffic streams, profiling can be derived from a variety of traffic perspectives, including profiles of • Protocol-specific transactions (e.g., all ICMP exchanges) • Sessions between specific internal hosts and/or specific external sites • Application-layer-specific sessions (e.g., anonymous FTP sessions profiled individually and/or collectively) • Discarded traffic, measuring attributes such as volume and disposition of rejections • Connection requests, errors, and unfiltered transmission rates and disposition Event records are generated either as a result of activity or at periodic intervals. In our case, activity records are based on the content of IP packets or transport-layer datagrams. Our event filters also construct interval summary records, which contain accumulated network traffic statistics (at a minimum, number of packets and number of kilobytes transferred). These records are constructed at the end of each interval (e.g., once per N seconds)." (pp. 6-7) "EMERALD uses volume analyses to help detect the introduction of malicious traffic, such as traffic intended to cause service denials or perform intelligence gathering, where such traffic

Claim number	Claim text	[illegible]
		may not necessarily be violating filtering policies. A sharp increase in the overall volume of discarded packets, as well as analysis of the disposition of the discarded packets (as discussed in Section 4.1, can provide insight into unintentionally malformed packets resulting from poor line quality or internal errors in neighboring hosts. High volumes of discarded packets can also indicate more maliciously intended transmissions such as scanning of UPD ports or IP address scanning via ICMP echoes. Excessive numbers of mail expansion requests (EXPN) may indicate intelligence gathering, perhaps by spammers. These and other application-layer forms of doorknob rattling can be detected by an EMERALD statistical engine when filtering is not desired." (p. 9) See Section 4.3 "Measuring Network Traffic Intensity" (pp. 9-10)
5	The method of claim 1, wherein the measure monitors network connections by monitoring network connection requests.	See '338 claim 1
6	The method of claim 1, wherein the measure monitors network connections by monitoring network connection requests.	See '338 claim 1
7	The method of claim 1, wherein the measure	See '338 claim 1

Claim Number	Claim Term	Corresponding Portion of Specification
	monitors network connections by monitoring network connection requests.	
8	The method of claim 1, wherein the measure monitors network connections by monitoring network connection requests.	See '338 claim 1
9	The method of claim 1, wherein the measure monitors network connections by monitoring network connection requests.	See '338 claim 1
10	The method of claim 1, wherein the measure monitors network connections by monitoring network connection requests.	See '338 claim 1
11	The method of claim 1, further comprising responding based on the	"In addition, we can add a layer of traffic-rate monitoring by profiling the overall volume of enterprise traffic expected throughout various slices of the day and week. Local monitors may use continuous measures to detect drastic declines in packet volumes that could indicate

	determining whether the difference between the short-term statistical profile and the long-term statistical profile indicates suspicious network activity.	transmission loss or serious degradation. However, it is conceivable that the degradation from the local domain perspective, while significant, is not drastic enough to warrant active response. At the same time, we may find through results correlation that the aggregate of all domains producing reports of transmission rate degradation during the same time period could warrant attention at the enterprise layer. Thus, local domain activity below the severity of warranting a response could in aggregation with other activity be found to warrant a response." (p. 14) "Within EMERALD, our response capabilities will employ the following general forms of response: • **Passive results dissemination:** EMERALD monitors can make their analysis results available for administrative review. We are currently exploring techniques to facilitate passive dissemination of analysis results by using already-existing network protocols such as SNMP, including the translation of analysis results into an intrusion-detection management information base (MIB) structure. However, whereas it is extremely useful to integrate results dissemination into an already-existing infrastructure, we must balance this utility with the need to preserve the security and integrity of analysis results. • **Assertive results dissemination:** Analysis results can be actively disseminated as administrative alerts. While the automatic dissemination of alerts may help to provide timely review of problems by administrators, this approach may be the most expensive form of response, in that it requires human oversight.[vi] • **Dynamic controls over logging configuration:** EMERALD monitors can perform

Claim number	Claim Element	[illegible]
		limited control over the (re)configuration of logging facilities within network components (e.g., routers, firewalls, network services, audit daemons). • **Integrity checking probes:** EMERALD monitors may invoke handlers that validate the integrity of network services or other assets. Integrity probes may be particularly useful for ensuring that privileged network services have not been subverted.[vii] • **Reverse probing:** EMERALD monitors may invoke probes in an attempt to gather as much counterintelligence about the source of suspicious traffic by using features such as *traceroute* or *finger*. However, care is required in performing such actions, as discussed in [4]. • **Active channel termination:** An EMERALD monitor can actively terminate a channel session if it detects specific known hostile activity. This is perhaps the most severe response, and care must be taken to ensure that attackers do not manipulate the surveillance monitor to deny legitimate access." (p. 15-16)
12	The method of claim 11, wherein responding comprises transmitting an event record to a network monitor.	"Another issue is how to tailor a response that is appropriate given the severity of the problem, and that provides a singular effect to address the problem without harming the flow of legitimate network traffic. Countermeasures range from very passive responses, such as passive results dissemination, to highly aggressive actions, such as severing a communication channel. Within EMERALD, our response capabilities will employ the following general forms of response: • **Passive results dissemination:** EMERALD monitors can make their analysis results available for administrative review. We are currently exploring techniques to facilitate passive dissemination of analysis results by using already-existing network protocols

		such as SNMP, including the translation of analysis results into an intrusion-detection management information base (MIB) structure. However, whereas it is extremely useful to integrate results dissemination into an already-existing infrastructure, we must balance this utility with the need to preserve the security and integrity of analysis results. • **Assertive results dissemination:** Analysis results can be actively disseminated as administrative alerts. While the automatic dissemination of alerts may help to provide timely review of problems by administrators, this approach may be the most expensive form of response, in that it requires human oversight.[vi]" (p. 16)
13	The method of claim 12, wherein transmitting the event record to a network monitor comprises transmitting the event record to a hierarchically higher network monitor.	"The focus of surveillance need not be limited to the analysis of traffic streams through a single gateway. An extremely useful extension of anomaly detection and signature analyses is to support the hierarchical correlation of analysis results produced by multiple distributed gateway surveillance modules. Within the EMERALD framework, we are developing meta-surveillance modules that analyze the anomaly and signature reports produced by individual traffic monitors dispersed to the various entry points of external traffic into local network domains. This concept is illustrated in Figure 1, which depicts an example enterprise network consisting of interconnected local network domains.[v] These local domains are independently administered, and could perhaps correspond to the division of computing assets among departments within commercial organizations or independent laboratories within research organizations. In this figure, connectivity with the external world is provided through one or more service providers (SP1 and SP2), which may provide a limited degree of filtering based on source address (to avoid address spoofing), as well as other primitive checks such as monitoring checksum." (p. 12)

Claim number	Claim Term	[illegible]
		See Figure: "Example Network Deployment of Surveillance Monitors" (p. 13) "EMERALD surveillance monitors are represented by the S-circles, and are deployed to the various entry points of the enterprise and domains. EMERALD surveillance modules develop analysis results that are then directed up to an enterprise-layer monitor, which correlates the distributed results into a meta-event stream. The enterprise monitor is identical to the individual gateway monitors (i.e., they use the same code base), except that it is configured to correlate activity reports produced by the gateway monitors. The enterprise monitor employs both statistical anomaly detection and signature analyses to further analyze the results produced by the distributed gateway surveillance modules, searching for commonalities or trends in the distributed analysis results. The following sections focus on aggregate analyses that may induce both local response and/or enterprise-wide response. We enumerate some of the possible ways that analysis results from the various surveillance modules can be correlated to provide insight into more global problems not visible from the narrow perspective of local entry-point monitoring." (p. 13-14)
14	The method of claim 13, wherein transmitting the event record to a network monitor comprises transmitting the event record to a network monitor that receives event records	See '338 claim 13

[illegible] number	[illegible]	[illegible]
	from multiple network monitors.	
15	The method of claim 14, wherein the monitor that receives event records from multiple network monitors comprises a network monitor that correlates activity in the multiple network monitors based on the received event records.	"More broadly, in Section 6 we discuss the correlation of analysis results produced by surveillance components deployed independently throughout the entry points of our protected intranet. We discuss how events of limited significance to a local surveillance monitor may be aggregated with results from other strategically deployed monitors to provide insight into more wide-scale problems or threats against the intranet." (p. 4) "On the other hand, event-distribution measures are useful in correlative analysis achieved via the ``Monitor of Monitors" approach. Here, each monitor contributes to an aggregate event stream for the domain of the correlation monitor. These events are generated only when the individual monitor decides that the recent behavior is anomalous (though perhaps not sufficiently anomalous by itself to trigger a declaration). Measures recorded include time stamp; monitor identifier, subject identifier, and measure identities of the most outlying measures. Overall intensity of this event stream may be indicative of a correlated attack. The distribution of which monitors and which measures are anomalous is likely to be different with an intrusion or malfunction than with the normal ``innocent exception." (See Section 6 for a further discussion on result correlation.)" (p. 10)
16	The method of claim 11, wherein responding comprises altering analysis of the network packets.	"Within EMERALD, our response capabilities will employ the following general forms of response: ... • **Dynamic controls over logging configuration:** EMERALD monitors can perform limited control over the (re)configuration of logging facilities within network components (e.g., routers, firewalls, network services, audit daemons).

		• **Integrity checking probes:** EMERALD monitors may invoke handlers that validate the integrity of network services or other assets. Integrity probes may be particularly useful for ensuring that privileged network services have not been subverted.[vii] • **Reverse probing:** EMERALD monitors may invoke probes in an attempt to gather as much counterintelligence about the source of suspicious traffic by using features such as *traceroute* or *finger*. However, care is required in performing such actions, as discussed in [4]." (p. 15-16)
17	The method of claim 11, wherein responding comprises severing a communication channel.	"**Active channel termination:** An EMERALD monitor can actively terminate a channel session if it detects specific known hostile activity. This is perhaps the most severe response, and care must be taken to ensure that attackers do not manipulate the surveillance monitor to deny legitimate access." (p. 16)
18	The method of claim 1, wherein the network packets comprise TCP/IP packets.	*"Specifically, we present techniques to analyze TCP/IP packet streams that flow through network gateways for signs of malicious activity, nonmalicious failures, and other exceptional events."* (Abstract)
19	The method of claim 1, wherein the network entity comprises a gateway, a router, or a proxy server.	In the following sections we discuss how such traffic streams can be statistically and heuristically analyzed to provide insight into malicious and erroneous external traffic. Alternative sources of event data are also available from the report logs produced by the various gateways, firewalls, routers, and proxy-servers (e.g., router syslogs can in fact be used to collect packet information from several products)." (pp. 4-5) "Within the EMERALD project, we generalize these concepts so that components and software such as network gateways, proxies, and network services can themselves be made subject classes. The generated event streams are obtained from log files, packet analysis, and--

[illegible] number	[illegible]	[illegible]
		where required--special-purpose instrumentation made for services of interest (e.g., FTP, HTTP, or SMTP). As appropriate, an event stream may be analyzed as a single subject, or as multiple subjects, and the same network activity can be analyzed in several ways. For example, an event stream of dropped packets permits analyses that track the reason each packet was rejected. Under such a scenario, the firewall rejecting the packet is the subject, and the measures of interest are the reason the packet was dropped (a categorical measure), and the rate of dropped packets in the recent past (one or more intensity measures tuned to time intervals of seconds to minutes). Alternatively, these dropped packets may be parsed in finer detail, supporting other analyses where the subject is, for example, the identity of the originating host." (p. 5)
21	A method of network surveillance, comprising:	See '338 claim 1
	monitoring network packets handled by a network entity;	See '338 claim 1
	building a long-term and multiple short-term statistical profiles of the network packets;	See '338 claim 1
	comparing one of the multiple short-term statistical profiles with the long-term statistical profile; and	See '338 claim 1

Claim number	Claim Limitation	[illegible]
	determining whether the difference between the one of the multiple short-term statistical profiles and the long-term statistical profile indicates suspicious network activity.	See '338 claim 1
22	The method of claim 21, wherein the multiple short-term monitoring statistical profiles comprise profiles that monitor different anonymous FTP sessions.	"Statistical anomaly detection via the methods described above enables EMERALD to answer questions such as how the current anonymous FTP session compares to the historical profile of all previous anonymous FTP sessions. Mail exchange could be similarly monitored for atypical exchanges (e.g., excessive mail relays). Continuing with the example of FTP, we assign FTP-related events to a subject (the login user or ``anonymous"). As several sessions may be interleaved, we maintain separate short-term profiles for each, but may score against a common long-term profile (for example, short-term profiles are maintained for each ``anonymous" FTP session, but each is scored against the historical profile of ``anonymous" FTP sessions). The aging mechanism in the statistics module allows it to monitor events either as the events occur or at the end of the session. We have chosen the former approach (analyze events as they happen), as it potentially detects anomalous activity in a session before that session is concluded." (p. 10)
23	The method of claim 21, wherein building multiple short-term statistical profiles comprise deinterleaving	See '338 claim 21.

[illegible]	[illegible]	[illegible]
	packets to identify a short-term statistical profile.	
24	A computer program product, disposed on a computer readable medium, the product including instructions for causing a processor to:	See '338 claim 1
	receive network packets handled by a network entity;	See '338 claim 1
	build at least one long-term and at least one short-term statistical profile from at least one measure of the network packets,	See '338 claim 1
	the measure monitoring data transfers, errors, or network connections;	See '338 claim 1
	compare at least one short-term and at least one long-term statistical profile; and	See '338 claim 1

Claim number	Claim text	[illegible]
	determine whether the difference between the short-term statistical profile and the long-term statistical profile indicates suspicious network activity.	See '338 claim 1

Claim number	Claim limitation	[illegible]
1	A computer-automated method of hierarchical event monitoring and analysis within an enterprise network comprising:	*"Specifically, we present techniques to analyze TCP/IP packet streams that flow through network gateways for signs of malicious activity, nonmalicious failures, and other exceptional events. The intent is to demonstrate, by example, the utility of introducing gateway surveillance mechanisms to monitor network traffic. We present this discussion of gateway surveillance mechanisms as complementary to the filtering mechanisms of a large enterprise network, and illustrate the usefulness of surveillance in directly enhancing the security and stability of network operations."* (Abstract) "Mechanisms for parsing and filtering hostile external network traffic [2],[4] that could reach internal network services have become widely accepted as prerequisites for limiting the exposure of internal network assets while maintaining interconnectivity with external networks. The encoding of filtering rules for packet- or transport-layer communication should be enforced at entry points between internal networks and external traffic. Developing filtering rules that strike an optimal balance between the restrictiveness necessary to suppress the entry of unwanted traffic, while allowing the necessary flows demanded for user functionality, can be a nontrivial exercise [3]." (p. 2) "Network monitoring, in the context of fault detection and diagnosis for computer network and telecommunication environments, has been studied extensively by the network management and alarm correlation community [8], [11], [15], [16]. The high-volume distributed event correlation technology promoted in some projects provides an excellent foundation for building truly scalable network-aware surveillance technology for misuse. ... Earlier work in the intrusion-detection community attempting to address the issue of network surveillance includes the Network Security Monitor (NSM), developed at UC Davis [6], and

[illegible] number	[illegible]	[illegible]
		the Network Anomaly Detection and Intrusion Reporter (NADIR) [7], developed at Los Alamos National Laboratory (LANL). Both performed broadcast LAN packet monitoring to analyze traffic patterns for known hostile or anomalous activity.[i] Further research by UC Davis in the Distributed Intrusion Detection System (DIDS) [23] and later Graph-based Intrusion Detection System (GRIDS) [25] projects has attempted to extend intrusion monitoring capabilities beyond LAN analysis, to provide multi-LAN and very large-scale network coverage." (p. 3) "We use the terms *enterprise* and *intranet* interchangeably; both exist ultimately as cooperative communities of independently administered domains, communicating together with supportive network infrastructure such as firewalls, routers, and bridges." (p. 18) "The focus of surveillance need not be limited to the analysis of traffic streams through a single gateway. An extremely useful extension of anomaly detection and signature analyses is to support the hierarchical correlation of analysis results produced by multiple distributed gateway surveillance modules. Within the EMERALD framework, we are developing meta-surveillance modules that analyze the anomaly and signature reports produced by individual traffic monitors dispersed to the various entry points of external traffic into local network domains." (p. 12)
	deploying a plurality of network monitors in the enterprise network;	"EMERALD introduces a building-block approach to network surveillance, attack isolation, and automated response. The approach employs highly distributed, independently tunable, surveillance and response monitors that are deployable polymorphically at various abstract layers in a large network. These monitors demonstrate a streamlined intrusion-detection design that combines signature analysis with statistical profiling to provide localized real-time protection of the most widely used network services and components on the Internet." (p. 3)

	detecting, by the network monitors, suspicious network activity	*"Specifically, we present techniques to analyze TCP/IP packet streams that flow through network gateways for signs of malicious activity, nonmalicious failures, and other exceptional events."* (Abstract)
	based on analysis of network traffic data selected from the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet};	"IP traffic represents an interesting candidate event stream for analysis. Individually, packets represent parsable activity records, where key data within the header and data segment can be statistically analyzed and/or heuristically parsed for response-worthy activity. However, the sheer volume of potential packets dictates careful assessment of ways to optimally organize packets into streams for efficient parsing. Thorough filtering of events and event fields such that the target activity is concisely isolated, should be applied early in the processing stage to reduce resource utilization. With respect to TCP/IP gateway traffic monitoring, we have investigated a variety of ways to categorize and isolate groups of packets from an arbitrary packet stream. Individual packet streams can be filtered based on different isolation criteria, such as • *Discarded traffic:* packets not allowed through the gateway because they violate filtering rules.[iii] • *Pass-through traffic:* packets allowed into the internal network from external sources. • *Protocol-specific traffic:* packets pertaining to a common protocol as designated in the packet header. One example is the stream of all ICMP packets that reach the gateway. • *Unassigned port traffic:* packets targeting ports to which the administrator has not assigned any network service and that also remain unblocked by the firewall.

		• *Transport management messages:* packets involving transport-layer connection establishment, control, and termination (e.g., TCP SYN, RESET, ACK, `[window resize]`). • *Source-address monitoring:* packets whose source addresses match well-known external sites (e.g., connections from satellite offices) or have raised suspicion from other monitoring efforts. • *Destination-address monitoring:* all packets whose destination addresses match a given internal host or workstation. • *Application-layer monitoring:* packets targeting a particular network service or application. This stream isolation may translate to parsing packet headers for IP/port matches (assuming an established binding between port and service) and rebuilding datagrams. In the following sections we discuss how such traffic streams can be statistically and heuristically analyzed to provide insight into malicious and erroneous external traffic. Alternative sources of event data are also available from the report logs produced by the various gateways, firewalls, routers, and proxy-servers (e.g., router syslogs can in fact be used to collect packet information from several products)." (pp. 4-5) "Within the EMERALD project, we generalize these concepts so that components and software such as network gateways, proxies, and network services can themselves be made subject classes. The generated event streams are obtained from log files, packet analysis, and--where required--special-purpose instrumentation made for services of interest (e.g., FTP, HTTP, or SMTP). As appropriate, an event stream may be analyzed as a single subject, or as

		multiple subjects, and the same network activity can be analyzed in several ways. For example, an event stream of dropped packets permits analyses that track the reason each packet was rejected. Under such a scenario, the firewall rejecting the packet is the subject, and the measures of interest are the reason the packet was dropped (a categorical measure), and the rate of dropped packets in the recent past (one or more intensity measures tuned to time intervals of seconds to minutes). Alternatively, these dropped packets may be parsed in finer detail, supporting other analyses where the subject is, for example, the identity of the originating host." (p. 5) "Through satellite session profiling, EMERALD can monitor traffic for signs of unusual activity. In the case of the FTP service, for example, each user who gives a login name is a subject, and "anonymous" is a subject as well. Another example of a subject is the network gateway itself, in which case there is only one subject. All subjects for the same event stream (that is, all subjects within a subject class) have the same measures defined in their profiles, but the internal profile values are different. As we migrate our statistical algorithms that had previously focused on user audit trails with users as subjects, we generalize our ability to build more abstract profiles for varied types of activity captured within our generalized notion of an event stream. In the context of statistically analyzing TCP/IP traffic streams, profiling can be derived from a variety of traffic perspectives, including profiles of • Protocol-specific transactions (e.g., all ICMP exchanges) • Sessions between specific internal hosts and/or specific external sites

[illegible] Claim Number	[illegible] Claim Limitation	[illegible] Prior Art Reference
		• Application-layer-specific sessions (e.g., anonymous FTP sessions profiled individually and/or collectively) • Discarded traffic, measuring attributes such as volume and disposition of rejections • Connection requests, errors, and unfiltered transmission rates and disposition Event records are generated either as a result of activity or at periodic intervals. In our case, activity records are based on the content of IP packets or transport-layer datagrams. Our event filters also construct interval summary records, which contain accumulated network traffic statistics (at a minimum, number of packets and number of kilobytes transferred). These records are constructed at the end of each interval (e.g., once per N seconds)." (pp. 6-7) See Section 4.1 "Categorical Measures in Network Traffic" (pp. 7-8) See Section 4.2 "Continuous Measures in Network Traffic" (pp. 8-9) See Section 4.3 "Measuring Network Traffic Intensity" (pp. 9-10) See Section 4.4 "Event Distribution Measures" (p. 10) See Section 4.5 "Statistical Session Analysis" (p. 10) See chart (p. 17-18)
	generating, by the monitors, reports of said suspicious activity; and	"The focus of surveillance need not be limited to the analysis of traffic streams through a single gateway. An extremely useful extension of anomaly detection and signature analyses is to support the hierarchical correlation of analysis results produced by multiple distributed gateway surveillance modules. Within the EMERALD framework, we are developing meta-surveillance modules that analyze the anomaly and signature reports produced by individual

[illegible] Claim Number	[illegible] Claim Limitation	[illegible] Prior Art Disclosure
		traffic monitors dispersed to the various entry points of external traffic into local network domains." (p. 12)
	automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.	"EMERALD surveillance modules develop analysis results that are then directed up to an enterprise-layer monitor, which correlates the distributed results into a meta-event stream. The enterprise monitor is identical to the individual gateway monitors (i.e., they use the same code base), except that it is configured to correlate activity reports produced by the gateway monitors. The enterprise monitor employs both statistical anomaly detection and signature analyses to further analyze the results produced by the distributed gateway surveillance modules, searching for commonalities or trends in the distributed analysis results. The following sections focus on aggregate analyses that may induce both local response and/or enterprise-wide response. We enumerate some of the possible ways that analysis results from the various surveillance modules can be correlated to provide insight into more global problems not visible from the narrow perspective of local entry-point monitoring." (p. 13-14)
2	The method of claim 1, wherein integrating comprises correlating intrusion reports reflecting underlying commonalities.	"On the other hand, event-distribution measures are useful in correlative analysis achieved via the ``Monitor of Monitors" approach. Here, each monitor contributes to an aggregate event stream for the domain of the correlation monitor. These events are generated only when the individual monitor decides that the recent behavior is anomalous (though perhaps not sufficiently anomalous by itself to trigger a declaration). Measures recorded include time stamp, monitor identifier, subject identifier, and measure identities of the most outlying measures. Overall intensity of this event stream may be indicative of a correlated attack. The distribution of which monitors and which measures are anomalous is likely to be different with an intrusion or malfunction than with the normal ``innocent exception." (See Section 6 for a further discussion on result correlation.)" (p. 10)

'205 Claim number	Claim Term	[illegible]
		"EMERALD surveillance modules develop analysis results that are then directed up to an enterprise-layer monitor, which correlates the distributed results into a meta-event stream. The enterprise monitor is identical to the individual gateway monitors (i.e., they use the same code base), except that it is configured to correlate activity reports produced by the gateway monitors. The enterprise monitor employs both statistical anomaly detection and signature analyses to further analyze the results produced by the distributed gateway surveillance modules, searching for commonalities or trends in the distributed analysis results. The following sections focus on aggregate analyses that may induce both local response and/or enterprise-wide response. We enumerate some of the possible ways that analysis results from the various surveillance modules can be correlated to provide insight into more global problems not visible from the narrow perspective of local entry-point monitoring." (p. 13-14) See Section 6.1 "Commonalities among Results" (p. 14)
3	The method of claim 1, wherein integrating further comprises invoking countermeasures to a suspected attack.	"In addition, we can add a layer of traffic-rate monitoring by profiling the overall volume of enterprise traffic expected throughout various slices of the day and week. Local monitors may use continuous measures to detect drastic declines in packet volumes that could indicate transmission loss or serious degradation. However, it is conceivable that the degradation from the local domain perspective, while significant, is not drastic enough to warrant active response. At the same time, we may find through results correlation that the aggregate of all domains producing reports of transmission rate degradation during the same time period could warrant attention at the enterprise layer. Thus, local domain activity below the severity of warranting a response could in aggregation with other activity be found to warrant a response." (p. 14)

		"Within EMERALD, our response capabilities will employ the following general forms of response: • **Passive results dissemination:** EMERALD monitors can make their analysis results available for administrative review. We are currently exploring techniques to facilitate passive dissemination of analysis results by using already-existing network protocols such as SNMP, including the translation of analysis results into an intrusion-detection management information base (MIB) structure. However, whereas it is extremely useful to integrate results dissemination into an already-existing infrastructure, we must balance this utility with the need to preserve the security and integrity of analysis results. • **Assertive results dissemination:** Analysis results can be actively disseminated as administrative alerts. While the automatic dissemination of alerts may help to provide timely review of problems by administrators, this approach may be the most expensive form of response, in that it requires human oversight.[vi] • **Dynamic controls over logging configuration:** EMERALD monitors can perform limited control over the (re)configuration of logging facilities within network components (e.g., routers, firewalls, network services, audit daemons). • **Integrity checking probes:** EMERALD monitors may invoke handlers that validate the integrity of network services or other assets. Integrity probes may be particularly useful for ensuring that privileged network services have not been subverted.[vii] • **Reverse probing:** EMERALD monitors may invoke probes in an attempt to gather as much counterintelligence about the source of suspicious traffic by using features such

[illegible] Claim number	[illegible] Claim Term	[illegible]
		as *traceroute* or *finger*. However, care is required in performing such actions, as discussed in [4]. **Active channel termination:** An EMERALD monitor can actively terminate a channel session if it detects specific known hostile activity. This is perhaps the most severe response, and care must be taken to ensure that attackers do not manipulate the surveillance monitor to deny legitimate access." (p. 15-16)
4	The method of claim 1, wherein the plurality of network monitors include an API for encapsulation of monitor functions and integration of third-party tools.	"EMERALD monitors can make their analysis results available for administrative review. We are currently exploring techniques to facilitate passive dissemination of analysis results by using already-existing network protocols such as SNMP, including the translation of analysis results into an intrusion-detection management information base (MIB) structure." (p. 16)
5	The method of claim 1, wherein the enterprise network is a TCP/IP network.	*"Specifically, we present techniques to analyze TCP/IP packet streams that flow through network gateways for signs of malicious activity, nonmalicious failures, and other exceptional events".* (Abstract)
6	The method of claim 1, wherein the network monitors are deployed at one or more of the following facilities of the enterprise network: {gateways, routers,	See '338 claim 19

	proxy servers).	
12	An enterprise network monitoring system comprising:	See '203 claim 1
	a plurality of network monitors deployed within an enterprise network;	See '203 claim 1
	said plurality of network monitors detecting suspicious network activity	See '203 claim 1
	based on analysis of network traffic data selected from the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in	See '203 claim 1

'615 Claim Number	'615 Claim Term	[illegible]
	a network packet);	
	said network monitors generating reports of said suspicious activity; and	See '203 claim 1
	one or more hierarchical monitors in the enterprise network, the hierarchical monitors adapted to automatically receive and integrate the reports of suspicious activity.	See '203 claim 1
13	The system of claim 12, wherein the integration comprises correlating intrusion reports reflecting underlying commonalities.	See '203 claim 2
14	The system of claim 12, wherein the integration further comprises invoking countermeasures to a suspected attack.	See '203 claim 3

Claim number	Claim text	Claim construction
15	The system of claim 12, wherein the plurality of network monitors include an application programming interface (API) for encapsulation of monitor functions and integration of third-party tools.	See '203 claim 4
16	The system of claim 12, wherein the enterprise network is a TCP/IP network.	See '203 claim 5
17	The system of claim 18, wherein a domain monitor associated with the plurality of service monitors within the domain monitor's associated network domain is adapted to automatically receive and integrate the reports of suspicious activity.	See '203 claim 6

Claim number	Claim language	Prior art publication
1	Method for monitoring an enterprise network, said method comprising the steps of:	See '203 claim 1
	deploying a plurality of network monitors in the enterprise network;	See '203 claim 1
	detecting, by the network monitors, suspicious network activity	See '203 claim 1
	based on analysis of network traffic data,	See '203 claim 1
	wherein at least one of the network monitors utilizes a statistical detection method;	"4. Traffic Analysis with Statistical Anomaly Detection SRI has been involved in statistical anomaly-detection research for over a decade [1], [5], [10]. Our previous work focused on the profiling of user activity through audit-trail analysis. Within the EMERALD project, we are extending the underlying statistical algorithms to profile various aspects of network traffic in search of response- or alert-worthy anomalies. The statistical subsystem tracks subject activity via one or more variables called *measures*. The statistical algorithms employ four classes of measures: categorical, continuous, intensity, and event distribution. *Categorical* measures are those that assume values from a categorical set, such as originating host identity, destination host, and port number. *Continuous* measures are those for which observed values are numeric or ordinal, such as number of bytes transferred. Derived measures also track the intensity of activity (that is, the rate of events per unit time) and the "meta-distribution" of the measures affected by recent events. These

Claim Number	Claim Term	Description
		derived measure types are referred to as *intensity* and *event distribution*. The system we have developed maintains and updates a description of a subject's behavior with respect to these measure types in a compact, efficiently updated *profile*. The profile is subdivided into short- and long-term elements. The short-term profile accumulates values between updates, and exponentially ages values for comparison to the long-term profile. As a consequence of the aging mechanism, the short-term profile characterizes the recent activity of the subject, where "recent" is determined by the dynamically configurable aging parameters used. At update time (typically, a time of low system activity), the update function folds the short-term values observed since the last update into the long-term profile, and the short-term profile is cleared. The long-term profile is itself slowly aged to adapt to changes in subject activity. Anomaly scoring compares related attributes in the short-term profile against the long-term profile. As all evaluations are done against empirical distributions, no assumptions of parametric distributions are made, and multi-modal and categorical distributions are accommodated. Furthermore, the algorithms we have developed require no *a priori* knowledge of intrusive or exceptional activity. A more detailed mathematical description of these algorithms is given in [9], [26]." (pp. 5-6)
	generating, by the monitors, reports of said suspicious activity; and	See '203 claim 1
	automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.	See '203 claim 1
2	The method of claim 1,	"Using basic signature-analysis concepts, EMERALD can support a variety of analyses

Claim number	Claim term	Evidence
	wherein at least one of the network monitors utilizes a signature matching detection method.	involving packet and transport datagrams as event streams. For example, address spoofing, tunneling, source routing [21], SATAN [27] attack detection, and abuse of ICMP messages (`Redirect` and `Destination` Unreachable) messages in particular) [4] could all be encoded and detected by signature engines that guard network gateways. The heuristics for analyzing headers and application datagrams for some of these abuses are not far from what is already captured by some filtering tools. In fact, it is somewhat difficult to justify the expense of passively monitoring the traffic stream for such activity when one could turn such knowledge into filtering rules.[iv]" (p. 11) See Section 5 "Traffic Analyzing with Signature Analysis" (pp. 10-12)
3	The method of claim 2, wherein the monitor utilizing a signature matching detection method also utilizes a statistical detection method.	*"We enumerate a variety of ways to extend both statistical and signature-based intrusion-detection analysis techniques to monitor network traffic."* (Abstract) "This paper takes a pragmatic look at the issue of packet and/or datagram analysis based on statistical anomaly detection and signature-analysis techniques. This work is being performed in the context of SRI's latest intrusion-detection effort, EMERALD, a distributed scalable tool suite for tracking malicious activity through and across large networks [20]. EMERALD introduces a building-block approach to network surveillance, attack isolation, and automated response. The approach employs highly distributed, independently tunable, surveillance and response monitors that are deployable polymorphically at various abstract layers in a large network. These monitors demonstrate a streamlined intrusion-detection design that combines signature analysis with statistical profiling to provide localized real-time protection of the most widely used network services and components on the Internet." (p. 3)